Policy Chapter:	**Chapter 14 Information Technology**
Policy Number and Title:	**14.003 Acceptable Use**

I. Policy Statement

The University of North Texas (UNT) provides Information Resources for employees, students, and authorized individuals to use in conducting official University business and for other purposes as authorized in this policy.

II. Application of Policy

This policy applies to all users granted access to University Information Resources, including but not limited to students, faculty, staff, and guests.

III. Policy Definitions

A. Access

"Access," in this policy, means the physical or logical capability to view, interact with, or otherwise make use of information resources.

B. Child[illegible]Cloud Service [illegible]

"Cloud Service," in this policy, means a service made available to a user by a third- party provider via the Internet in an externally managed data center or computing facility.

D. Confidential Information

"Confidential Information," in this policy, means information that must be protected from unauthorized disclosure or public release, based on state or federal law or other legal agreement (e.g., the Texas Public Information Act

, and other constitutional, statutory, judicial, and legal agreement requirements).

E. Data

"Data," in this policy, means all information, regardless of size or storage media, including email messages, system logs, and software (commercial or locally developed).

F. Email Domain

"Email Domain," in this policy, means the name used in an email address that identifies the organization to which the email is assigned or owned.

G. *Employee*

“Employee,” in this policy, means an individual who is employed full-time, part-time or in a temporary capacj0.0271 (acj03efs2)2 (-493 (p)1 (acj0.up)1 l271 (acj03(,)1 ()-51 (s)2 271 (a(p).13 (p

1. Authorized Use

3. Users must maintain the secrecy of their passwords. If a user suspects their password is compromised, they must reset it as soon as possible.
4. Users must report any misuse of Information Resources or violations of this policy to

c. injecting a virus or other malware into an Information Resource;

d. sending a message with the intent to disrupt University operations or the operations of outside entities;

e. printouts that tie up Information Resources for an unreasonable time period to the detriment of other authorized users;

f. sending spam messages;

g. computing tasks that consume an unreasonable amount of resources, either on or off campus, to the detriment of other authorized users; and

h. failing to adhere to usage limitations that apply at particular computer facilities on campus.

4. Use of University Information Resources for personal financial gain unrelated to University responsibilities and job expectations or for a personal commercial purpose.

5. Failure to protect the privacy of a password, account, or confidential information from unauthorized use or access.

6. Permitting someone to use another's account or credentials, or using someone else's account or credentials.

7. Unauthorized use, access, reading, or misuse of any electronic file, program, network, or system.

8. Unauthorized use, access, duplication, disclosure, alteration, damage, misuse, or destruction of data contained in any electronic file, program, network, or University hardware or software system.

9. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials. The unauthorized duplication and distribution of software and other materials protected by copyright (including copyrighted music, graphics etc.) is a violation of copyright law and this policy. Exceptions to this violation include specific authorization by the copyright holder or use protected by the fair use provisions of the copyright law.

10. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others through the use of institutionally owned Information Resources.

11. Attempting to circumvent, assisting someone else, or requesting that someone else circumvent any security measure or administrative access control that pertains to University data or Information Resources.

12. Use of University Information Resources in a manner that violates other University policies.

13. Use of University Information Resources for the transmission of commercial or personal advertisements, solicitations, or promotions in accordance with UNT's ethics policy.

14. Use of University Information Resources for transmission of political material in accordance with University's ethics policy.

15. Installing unauthorized software or hardware that permits unauthorized access to